

# 1. Engagement & Scope

## Objective

The primary objective of this Red Team Operation is to assess the security posture of the enterprise environment. The engagement aims to identify vulnerabilities, and misconfigurations in the AD environment and provide actionable recommendations for enhancing the security of the infrastructure.

## VPN Setup

VPN Credential

Username: KaiiZen

Password: q5Jal4jK

```
openvpn crtaKaiiZen.ovpn
2025-08-23 13:27:08 OpenVPN 2.6.14 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-08-23 13:27:08 library versions: OpenSSL 3.5.0 8 Apr 2025, LZO 2.10
2025-08-23 13:27:08 DCO version: N/A
Enter Auth Username: KaiiZen
Enter Auth Password: *****
2025-08-23 13:27:24 TCP/UDP: Preserving recently used remote address: [AF_INET]147.135.87.91:443
2025-08-23 13:27:24 Attempting to establish TCP connection with [AF_INET]147.135.87.91:443
2025-08-23 13:27:24 TCP connection established with [AF_INET]147.135.87.91:443
2025-08-23 13:27:24 TCPv4_CLIENT link local: (not bound)
2025-08-23 13:27:24 TCPv4_CLIENT link remote: [AF_INET]147.135.87.91:443
2025-08-23 13:27:25 WARNING: this configuration may cache passwords in memory -- use the auth-nocache option to prevent this
2025-08-23 13:27:25 [CCRTA-Lab] Peer Connection Initiated with [AF_INET]147.135.87.91:443
2025-08-23 13:27:27 TUN/TAP device tun0 opened
2025-08-23 13:27:27 net_iface_mtu_set: mtu 1500 for tun0
2025-08-23 13:27:27 net_iface_up: set tun0 up
2025-08-23 13:27:27 net_addr_v4_add: 10.10.200.225/24 dev tun0
2025-08-23 13:27:27 Initialization Sequence Completed
```

## Scope of engagement

Field	Value
VPN IP Range	10.10.200.0/24
External IP Range	192.168.80.0/24
Internal IP Range	192.168.98.0/24